

FOREWORD

The *Unified Build System Administrator's Guide* describes the setup and maintenance of Unified Build (UB) and also provides information about UB security administration in the GENSER and SCI environments.

This guide is divided into two sections: SYSADMIN Options and SECMAN Options. Each main section contains several subsections describing specific menu functions available under the specified user login.

SYSADMIN Options:

INTRODUCTION

Summarizes the JMCIS software environment and installation configurations. Provides additional sources of information. 5

SYSTEM ENVIRONMENT

Describes the hardware requirements and operating system. 9

OPERATING GUIDELINES

Explains startup and shutdown of the software and hardware, and lists database limits for various UB files. 15

SYSTEM ADMINISTRATION UTILITIES

Describes the functions available to a sysadmin user account, such as data backup and system reboot. 21

COMMUNICATIONS

Provides information about networks, physical interfaces to the system, communications and broadcast configuration and troubleshooting. 55

ERROR RECOVERY GUIDELINES

Describes potential problems, errors, and solutions. 77

SECMAN Options:

INTRODUCTION

Summarizes the security menu screen. 85

SYSTEM MENU

Options to set menu font size for the security application and to exit the system. 87

SECURITY MENU

Options to update audit status, review audit information and archive
audit logs..... 91

ACCOUNTS MENU

Options to create, edit, review, maintain, archive, restore, and export
roles and user accounts..... 101

PRINTING

Creating and using printers. 115

SYSADMIN OPTIONS

(This page has been intentionally left blank.)

CHAPTER 1: SYSADMIN INTRODUCTION

The SYSADMIN portion of this guide describes the setup and maintenance UB. Unified Build was derived from the Joint Operational Tactical System (JOTS)– a command and control system originally designed for the afloat Navy.

The following chapters describe menus and options available on the menu bar under the SYSADMIN login.

SYSTEM ENVIRONMENT

Describes the hardware requirements and operating system. 9

OPERATING GUIDELINES

Explains startup and shutdown of the software and hardware, and lists database limits for various UB files. 15

SYSTEM ADMINISTRATION UTILITIES

Describes the functions available to a sysadmin user account, such as data backup and system reboot. 21

COMMUNICATIONS

Provides information about networks, physical interfaces to the system, communications and broadcast configuration and troubleshooting. 55

ERROR RECOVERY GUIDELINES

Describes potential problems, errors, and solutions. 77

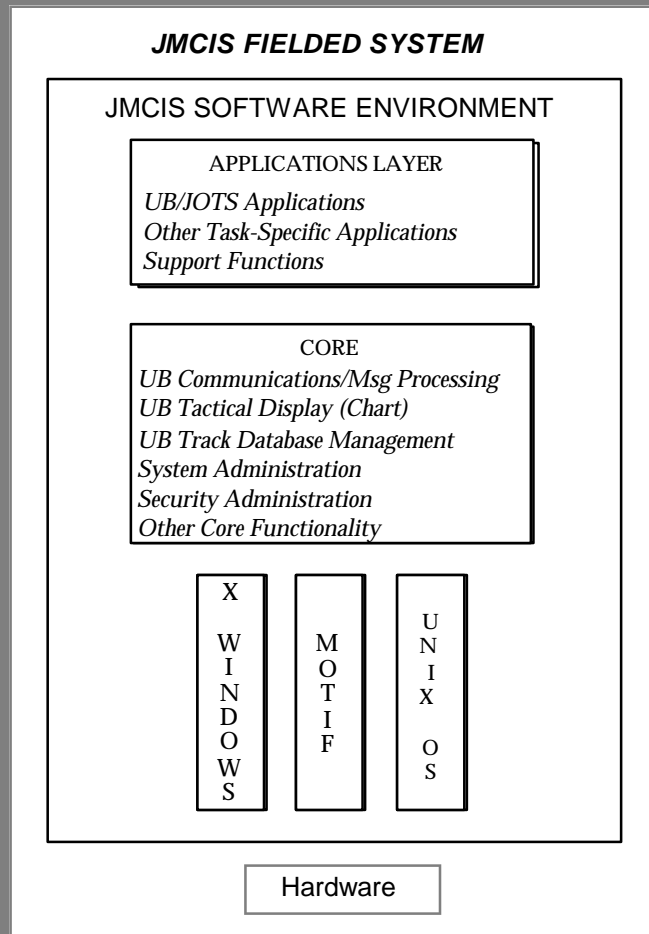


Figure 1-1 Core Components of JMCIS

1.1.1 INSTALLATION CONFIGURATIONS

When JMCIS operates in standalone configuration, all functions are performed on a single workstation. The standalone configuration is typically used for intelligence applications for which security restrictions, such as discretionary access controls, may preclude the typical network configuration.

When multiple workstations are configured on a local area network (LAN), typical system configuration consists of one workstation serving as communications

processor (CP) and track database manager and all others acting as clients. The server provides the shared tactical picture for the LAN.

Workstations on a LAN may also be configured as a combination of work groups and standalone machines. Each JMCIS work group operates as a separate LAN, with one workstation in the group acting as server and all others acting as clients.

For details on installation configuration, see Chapter 4, *System Installation*.

1.1.2 JMCIS FUNCTIONALITY

The functions described in this document may not correspond with those available on a particular workstation. Factors that determine the availability of functions include:

- LAN classification
- workstation classification
- user's account group, role, and classification

1.2 ADDITIONAL SOURCES OF INFORMATION

JMCIS Security Manager's Guide— explains security administration functions, including user accounts and roles.

JMCIS System Administrator's Guide— provides information regarding configuration, installation, and troubleshooting for all JMCIS segments, including NIPS, TIMS, NIEWS, etc.

Unified Build Training Manual— a self-paced tutorial on basic system components.

Unified Build User's Guide— describes each menu option within the JMCIS COE, JMCIS Applications, and Printer segments.

Other task-specific applications are described in separate documents.

Notes

CHAPTER 2: SYSTEM ENVIRONMENT

Host computers for the current JMCIS software suite are:

- TAC-3/4 (Tactical Advanced Computer, version 3)
- RSC-1X/2X (Gray Box)
- Sparc 10/20

2.1 HARDWARE COMPONENTS

The software uses one hard disk for the UNIX-based operating system and all core applications. If necessary, the second hard disk is used to load additional segments and to store data elements, such as extra map data.

2.1.1 TAC-3/4 HARDWARE

- HP 9000/7xx, with 64–192 MB of RAM
- *at least* one 1.2 GB hard disk drive
- 1.2-2.0 GB DAT drive (required to install the software)
- monitor
- HP keyboard
- HP trackball
- 1–2 graphics boards, each with 1–2 outputs
- two serial ports

Optional

- color large screen display (CLSD)
- floppy disk drive
- cartridge tape drive
- 5 GB, 8 mm Exabyte tape drive
- Sun keyboard and trackball with HP/Sun keyboard interface assembly*
- CD ROM
- EISA audio card (Pro AudioSpectrum or Pro AudioStudio)
- 8 or 16 port multiplexers (MUX) (Danford or Equinox) for Sun keyboards only

*To allow distant remote configurations, standard shipboard installations are delivered with a Sun keyboard and trackball, rather than HP. An HP keyboard is required to install the operating system tape, but the Sun keyboard and trackball are used to install segments and run the system.

2.1.2 RSC GRAY BOX COMPONENTS

- Sun IPX CPU, with 64 MB of RAM
- S-BUS to VME bus interface
- one 1.2 GB hard disk drive (optional if an RSC-2X is connected)
- floppy disk drive
- 10.4-inch monitor (used optionally with a second display)
- Sun-4 compatible keyboard
- 3-button trackball
- DAT drive
 - external (RSC-1X)
 - internal (RSC-2X)
- 1.2 GB hard disk drive
 - one (either 1X or 2X)
 - two (one in each)
- CD ROM (RSC-2X)

2.1.3 SPARC 10/20 HARDWARE

- Sun Sparc10/20 with 64–192 MB of RAM
- *at least* one 1.2 GB hard disk drive
- 1.2-2.0 GB *Sun* DAT drive (required to install the software)
- CD ROM
- monitor
- Sun keyboard
- Sun trackball
- 1–2 graphics boards, each with 1–2 outputs
- two serial ports

Optional

- color large screen display (CLSD)
- floppy disk drive
- cartridge tape drive
- 5 GB, 8 mm Exabyte tape drive

2.2 MULTI-MONITOR CONFIGURATIONS

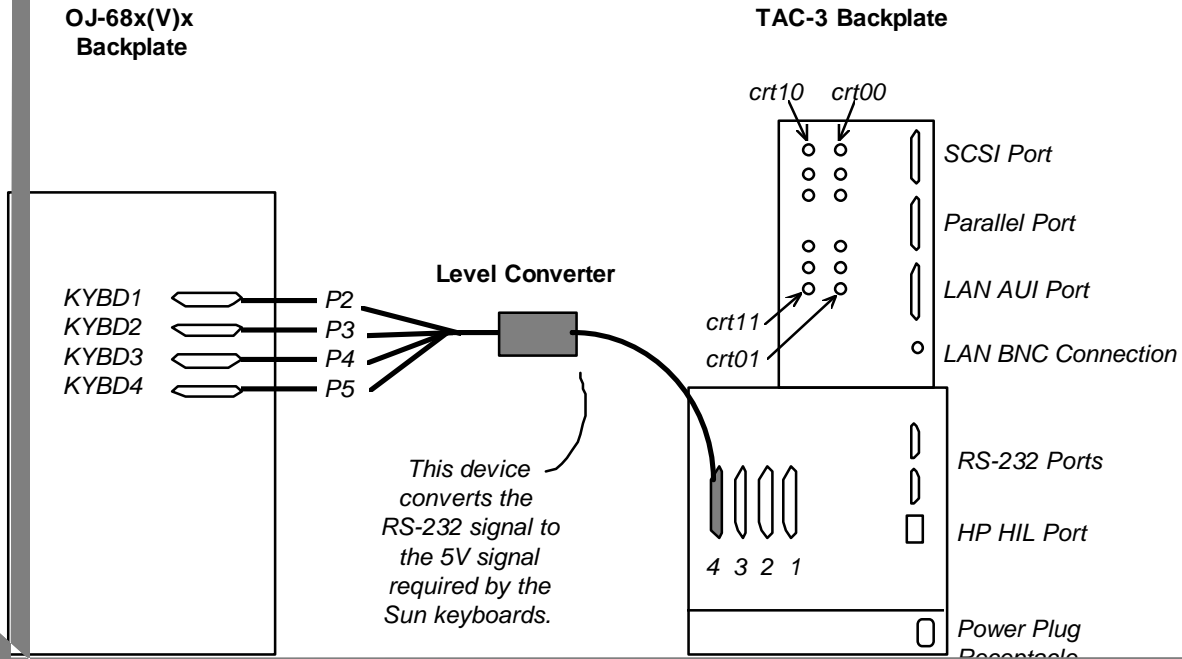
A single, properly equipped TAC-3 CPU can drive any of the following configurations:

- a single-eye console with 1–3 single-eye remote monitors
- a dual-eye console with 1–2 single-eye remote monitors
- a dual-eye console with a dual-eye remote monitor

Keyboards

- If an HP keyboard is used, only a single-eye console with *no* remote monitors may be set up. (The HP keyboard is connected via the HIL port.)
- For multi-monitor configurations, Sun keyboards *must* be used.
- The HP and Sun keyboards should *not* be connected to the CPU at the same time.

Figure 2-1 shows the rear view of a standard TAC-3 CPU. Ports in the multi-monitor connection scheme are indicated.



Single-Eye Console	Remote 1	Remote 2	Remote 3
Monitor: crt00 Keyboard: KYBD4	None	None	None
Monitor: crt00 Keyboard: KYBD1	Single-eye Monitor: crt01 Keyboard: KYBD2	None	None
Monitor: crt00 Keyboard: KYBD1	Single-eye Monitor: crt01 Keyboard: KYBD2	Single-eye Monitor: crt10 Keyboard: KYBD3	None
Monitor: crt00 Keyboard: KYBD1	Single-eye Monitor: crt01 Keyboard: KYBD2	Single-eye Monitor: crt10 Keyboard: KYBD3	Single-eye Monitor: crt11 Keyboard: KYBD4

Dual-Eye Console

Dual-Eye Console	Remote 1	Remote 2
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	None	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	Single-eye Monitor: crt10 Keyboard: KYBD4	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	Single-eye Monitor: crt10 Keyboard: KYBD3	Single-eye Monitor: crt11 Keyboard: KYBD4
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	Dual-eye Top Monitor: crt11 Bottom Monitor: crt10 Keyboard: KYBD3	None

For potential difficulties the user may encounter in a multi-monitor environment, see *Troubleshooting Multi-monitors* in Chapter 6.

2.3 THE JMCIS OPERATING SYSTEM (OS)

The JMCIS OS is a modified version of the UNIX OS, which accompanies the original hardware.

The JMCIS OS tape contains software relating to four areas:

- The operating system.
- The administration software required for installation, and for system and security administration.
- X Windows software.
- Motif software.

When a change is required in one or more of these areas, a new tape is built and the version number is increased by one. Thus, a change in the JMCIS OS tape may not be— and in fact is usually not— the result of a change to the “operating system.”

Notes

CHAPTER 3: OPERATING GUIDELINES

3.1 POWER DOWN

- *Never* power down the system without first executing a shutdown, as described below. Doing so could cause irreparable damage.
 - If the system has already been brought down improperly, refer to Chapter 6, *Error Recovery*.
1. Select EXIT from the SYSTEM menu in the main menu bar.
 2. Log in with a sysadmin account and password.
 3. Select SHUTDOWN SYSTEM from the HARDWARE menu.
 4. Wait until the following message appears: “syncing file systems... done. Halted.”
 5. Turn off the peripherals, including the monitor.
 6. Turn off the computer.

3.2 POWER UP

1. Turn on the Uninterruptable Power Supply (UPS) if necessary.
2. Turn on the peripherals, including the monitor.
3. Turn on the computer.
4. Enter assigned login and password at the prompts. The machine name is displayed in the login window.

3.3 DATABASE SIZE LIMITS

<i>TRACKS</i>	<i>LIMITS</i>
Platform/Ambiguity	1500
Emitter	1500
Link	1024
Acoustic	100
Unit	500
SPA-25G	400
RAYCAS	50
SI	450
FCS	100
External	0
Total 5624 (Max 6774)	

<i>OTHER TRACK RANGES</i>	<i>LIMITS</i>
Confidence Level of AOU Cross-fix Ellipse	90%
Dynamic Status Board	1 master track / 20 slave tracks
Land Sites	100
Missile Systems/track	10
Radar Systems/track	10
Sonar Systems/track	10
Weapon Systems/track	10
Specific IFF Mode-2 Valued Tracks Can Be Archived	20
Specific NTDS Track Numbers Can Be Archived	20
Track Archive Sequence of Steps	60 seconds
Track Groups	32
Tracks/group	Limited only by disk storage
Track History Reports/track	1,000
Track Symbol Label	26 characters
Tracks JMIE Database Will Send	10

<i>COMMUNICATIONS</i>	<i>LIMITS</i>
------------------------------	----------------------

(V) 6 Queue	50 messages
Addressee (Channel Message Buffer Manager)	1,000 backlog messages
Alert Log	1,000 messages
Incoming Message Log	1,000 messages
Incoming Opnote Log	200 opnotes
Outgoing Message Log	1,000 messages
RAINFORM Messages	1,000 lines
Received Messages Displayed in Status Window	1,000 messages
Report Log	2,000 reports
Saved for Raw Messages	500 lines

MISC	LIMITS
Auto-Forwarding, Addresses	500
Broadcast, User-Set Cycle Rate	0-720 minutes
Broadcasts, Active	25
Characters Stored per Screen Name	50
Clipboard, Files Stored on	1,000
Engagement Scenarios	10
Grid Cells, Number of	24 or 48
HULTEC Database	650
IFF/DIs, Nicknames	100
Incoming Message Alert, Addresses	5
Incoming Message Alert, Originators	5
Net Address (DDN)	256
PIM Tracks	100
PIM Track Legs	256
SAR Patterns in SAR Database	20
Satellite Charlie Elements	300
Satvul-Satellites per Category	300
Screen-Kilo Formations	100
Screen-Kilo, Ships per Formation	50
Stored Screen, Briefing Slides	50
Stored Screens, Number of	50
4-Whiskey Formations	100
4-Whiskey, Ships per Formation	50

MAPS	LIMITS
-------------	---------------

Key Sites	1,000
ROTHR Display of RTN on Map	15 characters
Stored Map, Parameter Combinations	500
Stored Maps	20
Zoom Width, Greatest	21,600 NM
Zoom Width, Smallest	0.25 NM
<i>OVERLAYS</i>	
Overlay, Items	100
Overlay, Points	256
Overlay, Polyline Points	256
Overlays, Number of	500

Notes

Notes

CHAPTER 4:

SYSTEM ADMINISTRATION UTILITIES

The sysadmin user account accesses the JMCIS system administration and maintenance utilities. These utilities perform functions such as making a backup data tape, restoring data to the system from a backup tape, changing the machine unique ID, and other administrative tasks.

Log in with the sysadmin user account from the GCCS login screen and the system displays a menu bar containing main menu items of the following:

- SYSTEM (Section 4.1)
- HARDWARE (Section 4.2)
- SOFTWARE (Section 4.3)
- DATABASE (Section 4.4)
- NETWORK (Section 4.5)

From these main menus, pull-down menus provide the system administrator with the functions necessary to maintain the system.

4.1 SYSTEM MENU

The System menu provides utilities to assist in controlled power-up and shutdown of the system. The following options are available from the System menu:

Find Launch

To automatically locate the LAUNCH WINDOW on the desktop.
(Section 4.1.1)

Stop Program

To kill a running application process. (Section 4.1.2)

Print Screen

To print a hardcopy version of the workstation screen as it currently appears. (Section 4.1.3)

Select Printer

To assign a default printer to the workstation. (Section 4.1.4)

System Status

To check the status of GCCS on the local network. (Section 4.1.5)

Restart

To immediately begin the reboot procedure. (Section 4.1.6)

Power Down

To execute a shutdown command, allowing the computer to be powered off without damaging the operating system. (Section 4.1.7)

Close All

To immediately close all open GCCS windows. (Section 4.1.8)

Logout

To exit the System Administration function and return to the GCCS Login prompt. (Section 4.1.9)

4.1.1 FIND LAUNCH

In GCCS, the LAUNCH window is provided to allow easy access to the installer, xterms, and the printer. The LAUNCH window appears when you login as the system administrator, and may be iconified in the same manner as any GCCS window.

Should you, at some point, iconify or layer the LAUNCH window beneath another window, selecting Find Launch opens the LAUNCH window, layering it over any other windows so it is fully visible.

4.1.2 STOP PROGRAM

The Stop Program option allows you to kill any application process by choosing it from a list of running processes that is displayed in the Stop Program window.

To stop a program:

1. Select Stop Program. The Stop Program window appears.



Figure 4-1 Stop Program Window

2. The Running Program: field displays a list of currently active processes. Click on the entry in the Running Program: field that corresponds to the process you wish to stop. The process you selected is now displayed in the Program to Stop: field.
3. Click Apply to apply the deletion to the process. A warning window appears, informing you that this process is destructive and should only be used to kill a hung process.
4. Click OK in the warning window to stop the program and return to the Stop Program window (or click CANCEL to dismiss the window and return to the Stop Program window).
5. Click OK in the Stop Program window to dismiss it (or click CANCEL).

4.1.3 PRINT SCREEN

The Print Screen option provides a method to capture the windows displayed on the workstation monitor and print them to hardcopy on the workstation default printer.

To print a screen:

1. Select Print Screen. The Print Screen window appears.

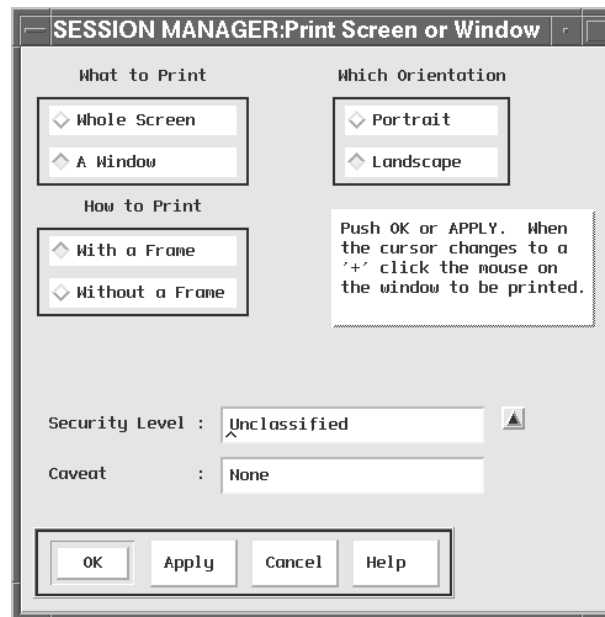


Figure 4-2 Print Screen Window

2. Select the appropriate diamond knob in the What to Print:, Which Orientation:, and How to Print: boxes. The Remarks box below the Which Orientation: box provides any instructions for additional steps you may need to perform in accordance with your selections.

3. Select the appropriate security level by clicking the list box to the right of the Security Level: field and choosing the corresponding entry. This marking will appear as a header and footer on the printed page.
4. Enter any remarks you want to appear on the hardcopy (i.e., a short description, etc.) into the Comment: field.
5. Click OK or Apply to print your selection to the workstation's default printer.

4.1.4 SELECT PRINTER

The Select Printer option allows you to assign a default printer to the workstation.

To select a printer:

1. Select Select Printer. The Select Printer window appears.

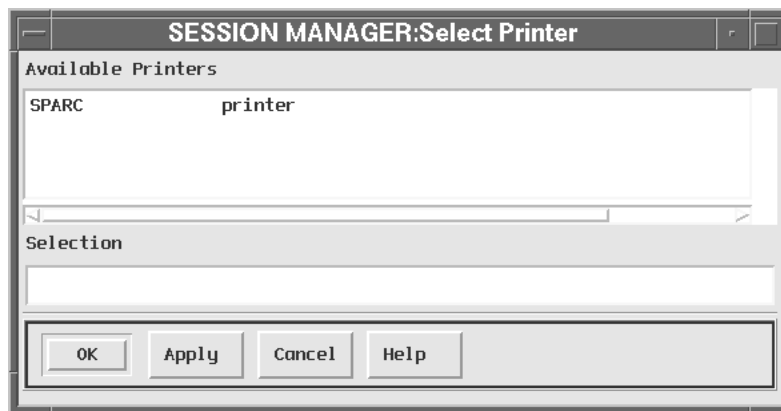


Figure 4-3 Select Printer Window

2. The Available Printers: field displays a list of currently available printers. Click on the entry in the Available Printers: field that corresponds to the printer you wish to assign to the default. The printer you selected is now displayed in the Selection: field.
3. Click Apply to apply the selection.
4. Click OK in the Select Printer window to accept the assignment and dismiss the Select Printer window.

4.1.5 SYSTEM STATUS

The System Status option provides a method to view the current status of GCCS nodes on the local network.

To view the system status:

1. Select System Status. The System Status window appears.

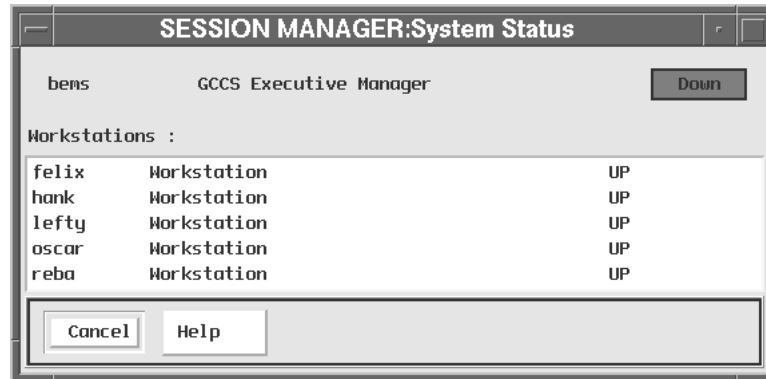


Figure 4-4 System Status Window

2. The System Status window displays a list of known nodes (hosts) on the GCCS and their status (UP or DOWN).
3. Click OK to dismiss the System Status window.

4.1.6 RESTART

The Restart option allows you to reboot the operating system. After selecting RESTART, you are asked to confirm the reboot. Click YES to continue.

The reboot process usually takes about six minutes, during which the screen appears gray and then black. When the process is complete, the Login window appears.

4.1.7 POWER DOWN

It is very important that the system never be powered off using the ON/OFF switch without first executing a shutdown. This could be very harmful to the system. If the system has already been brought down unnaturally, refer to Chapter 6 in this guide.

The power-down sequence is as follows:

1. Login as **sysadmin**.
2. Select POWER DOWN from the SYSTEM ADMINISTRATION menu.
3. Wait until this message appears on the system console:
"synching file systems... done"
"Halted."

4. Power down the hardware.

4.1.8 CLOSE ALL

The Close All option closes all open GCCS windows, dismissing them immediately.

4.1.9 LOGOUT

Select the Logout option to exit the SYSADMIN function and return to the GCCS login screen.

4.2 HARDWARE MENU

The Hardware menu provides utilities to assist in the maintenance of a satisfactory software/hardware interface. The Hardware menu presents the following options:

Shutdown System

To shut down the operating system properly, allowing the computer to be powered off. (Section 4.2.1)

Reboot System

To reboot the operating system with a disk check. (Section 4.2.2)

Disk Manager

To display available mounted and unmounted devices and file systems, such as sd0a, sd1h, and /home/Nauticus/data/mnt. (Section 4.2.3)

Config Printer

To configure a printer for a particular machine and port, and define remote access for the printer on the LAN. (Section 4.2.4)

4.2.1 SHUTDOWN SYSTEM

Use the SHUTDOWN SYSTEM option to shut down the operating system properly, allowing the computer to be powered off.

4.2.2 REBOOT SYSTEM

Use the REBOOT SYSTEM option to reboot the operating system with a disk check.

4.2.3 DISK MANAGER

The Disk Manager option provides information on the available mounted and unmounted devices and file systems on a workstation, such as sd0a, sd1h, and /home/Nauticus/data/mnt.

- A *mounted* device can be accessed for read and write operations.
- An *unmounted* device has disk space that is potentially available for such operations. An unmounted device must be mounted to a particular directory before its available space can be used.

To view this data, select the Disk Manager option from the Hardware menu. The Disk Manager window appears.

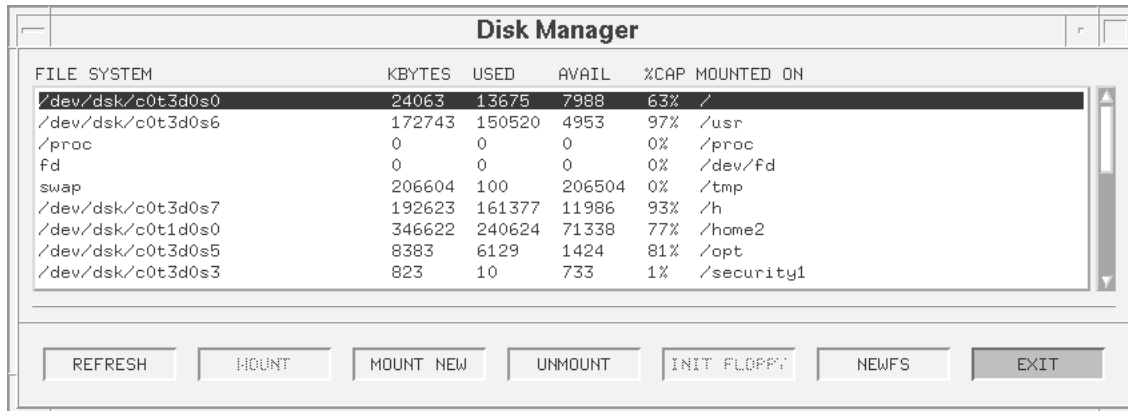


Figure 4-5 Disk Manager Window

To mount a device:

Note: Problems may arise if two devices are mounted to the same directory. To prevent this, ensure that no duplicate references to the same directory exist in the MOUNTED ON column.

1. Select the device name to mount and then click MOUNT. (Note that a pop-up menu is available with SELECT ALL and UNSELECT ALL options.)
2. Respond to the prompt, Do you need a permanent mount? Click OK for a permanent mount.
3. Click EXIT to exit the Disk Manager window.

To unmount a device:

Select the device name to unmount and then click UNMOUNT.

To mount a new device:

Note: Problems may arise if two devices are mounted to the same directory. To prevent this, ensure that no duplicate references to the same directory exist in the MOUNTED ON column.

1. Click MOUNT NEW. The MOUNT FILE SYSTEM window appears.

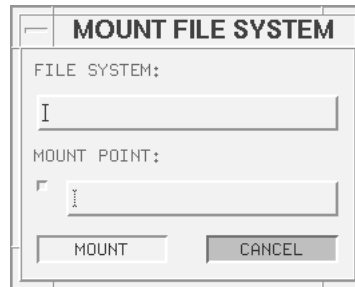


Figure 4-6 MOUNT FILE SYSTEM Window

2. In the FILE SYSTEM field, enter the pathname of the remote file system that you wish to mount on your local machine.
3. In the MOUNT POINT field, enter the pathname of the directory where you would like the remote file system mounted. You may choose from a list of directories on your machine by typing in the directory name or by clicking the knob to the left of the MOUNT POINT field and selecting the desired directory from the list presented in the CHOOSE MOUNT POINT window.
4. Click MOUNT to mount the file system to the designated mount point directory on your machine.

Note: The other buttons in the Disk Manager window are not currently functional. They will be activated and documented in a future release of the software.

4.2.4 CONFIG PRINTER

The CONFIG PRINTER option configures a printer for a particular machine and port, and defines remote access for the printer on the LAN.

To view the printer configuration:

Select Config Printer. The PRINTER SETUP window appears.

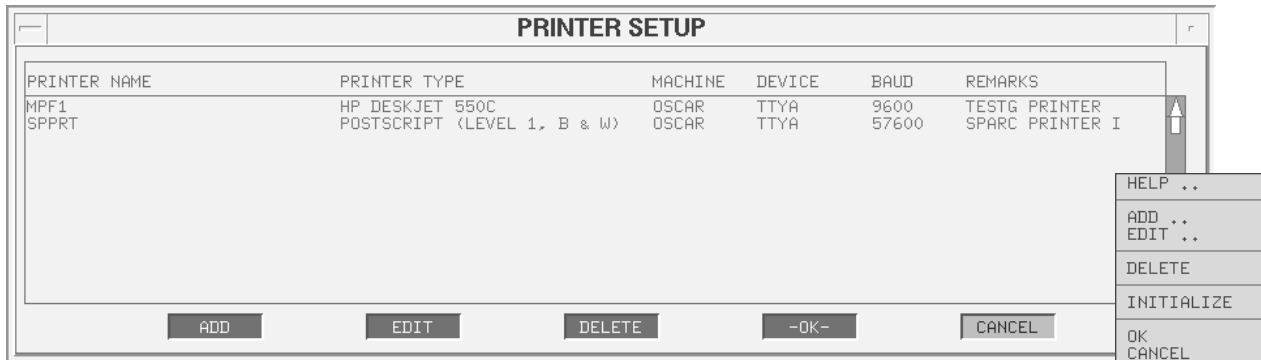


Figure 4-7 PRINTER SETUP Window

When the PRINTER SETUP window is *first* opened, no printers are available on the network. If a list of printer names appears in the window, some other printer configuration was previously implemented.

Important considerations for configuring printers:

- A list of the printers supported by GCCS is available.
- You may define which workstations have access to each printer.
- After making any changes to the printer setup—add, edit, or delete— you must initialize to set the printer configuration. See the example below for detailed information on the INITIALIZE procedure.

The ADD, EDIT, DELETE, OK, and CANCEL buttons operate in the standard manner.

To add a new printer:

1. In the PRINTER SETUP window, click ADD. The ADD NEW PRINTER window appears.



Figure 4-8 ADD NEW PRINTER Window

2. Click in the PRINTER NAME field and enter the name of the printer.
3. Click the list box next to the PRINTER TYPE: field to display the list of supported printers.
4. Click the appropriate entry in the list to display it in the PRINTER TYPE field.
5. Click the list box next to the HOST MACHINE field for a list of available hosts on the LAN. Double-click the entry to select the list entry which corresponds with the hostname of the machine where the printer is physically attached to the network. The selected hostname appears in the HOST MACHINE field.
6. Click the list box next to the DEVICE field for a list of available ports on the workstation. Double-click the entry to select the list entry which corresponds with the port you wish to use for the printer. The selected device appears in the DEVICE field.
7. Enter additional information, such as the printer's physical location, into the REMARKS field.
8. Click the checkbox beside the USE EXISTING LOCAL UNIX PRINTER field to place an X in the checkbox.

Note: The USE EXISTING LOCAL UNIX PRINTER setting should be used if the printer being enabled already exists in UNIX (e.g., a SPARCPrinter that has been created with the NeWSprint software). Checking this box will prevent UB from modifying the UNIX printer, and will simply allow UB to print to it. If you do not check this box before initializing the UB printer, any UB printer which uses a duplicate of a UNIX printer name will delete the UNIX printer and re-initialized it as a UB printer.

9. Click checkboxes in the AUTHORIZED REMOTE ACCESS box to enable remote printing from other machines on the LAN. Place an X in the checkbox corresponding to each machine with permission to use the printer.
10. Click OK to return to the PRINTER SETUP window with the new data. (Clicking CANCEL would ignore the new printer data.)
11. Select INITIALIZE from the pop-up menu for the PRINTER SETUP window to update the applicable JMCIS printer tables and set the printer configuration.

The INITIALIZE option must be performed individually on every workstation after you add, edit, or delete printers from the network configuration. The new configuration will not be available to any workstation which has not performed this step.

Note: The initialization step must be performed before the PRINTER SETUP window is dismissed. Failure to initialize will result in the loss of the new configuration information when the PRINTER SETUP window is closed.

12. Click OK at the “Save and Initialize These Printer Choices” prompt. When the initialize process is complete, you are returned to the PRINTER SETUP window.

To edit a printer entry:

1. In the PRINTER SETUP window, select the printer you wish to edit and click EDIT. The EDIT PRINTER window appears.
2. The EDIT PRINTER window fields function like those of the ADD PRINTER window. See the description above.

To delete a printer:

In the PRINTER SETUP window, select the printer entry you wish to delete and click DELETE. The printer entry is deleted.

4.3 SOFTWARE MENU

The Software menu provides utilities to assist in the maintenance and upgrade of the software loaded on a workstation as well as its connection to the LAN. The Software menu provides the following options:

Segment Installer

To load software segment from DAT tape. (Section 4.3.1)

Installation Server

To “load” segments for remote installation across the network.
(Section 4.3.2)

Archive Net Server

To archive network information on software installed on the comms server. (Section 4.3.3)

Restore Net Server

To restore network data to comms server. (Section 4.3.4)

Enable GenBroadcast

To activate a GEN Broadcast. (Section 4.3.5)

Disable GenBroadcast

To disable a GEN Broadcast. (Section 4.3.6)

The following is not a Software menu option, but deals with the networking and software configuration on a workstation.

Adding a New NIS+ Client (Solaris)

To set up an NIS+ client workstation. (Section 4.3.7)

4.3.1 SEGMENT INSTALLER

All GCCS software is packaged in modules called software segments. These segments are loaded using the Segment Installer tool. The Segment Installer tool is a Graphical User Interface (GUI) that does the following:

- Identifies which applications/segments are loaded on your system.
- Identifies which applications/segments are available on a tape or on a Segment Installation Server.
- Provides the capability to install and/or de-install applications/segments on the system.

The Segment Installer installs software in the /h file system. When this file system is approximately 80 percent full, the Segment Installer will install software in /home1, followed by /home2, /home3, . . . , /home99. The 80 percent constraint can be overridden on systems with limited amounts of disk space by using the Disk Space Override feature of the Segment Installer.

In most cases, the software installation process is automatic, requiring no further actions on the part of the installer.

All segments are contained on 4mm or 8mm tapes provided by DISA.

To install GCCS applications:

1. At the GCCS Workstation Console Login: prompt, enter sysadmin and press [Return].
2. At the Password: prompt, enter the sysadmin password (default vinson) and press [Return].
3. Agree to the provisions set forth in the Consent to Monitoring screen by pressing [Return]. The SYSTEM ADMINISTRATOR screen appears.
4. Insert the tape containing the segment into the DAT drive and wait until the control panel LEDs stop blinking.
5. From the Software pull-down menu, select Segment Installer. The System Processing Warning window appears, displaying any sessions that are

- To terminate all active sessions, click OK. The SEGMENT INSTALLER window appears.



- Click **SELECT MEDIA** in the upper portion of the **SOURCE** box in the **SEGMENT INSTALLER** window. The **SELECT MEDIA** window appears.

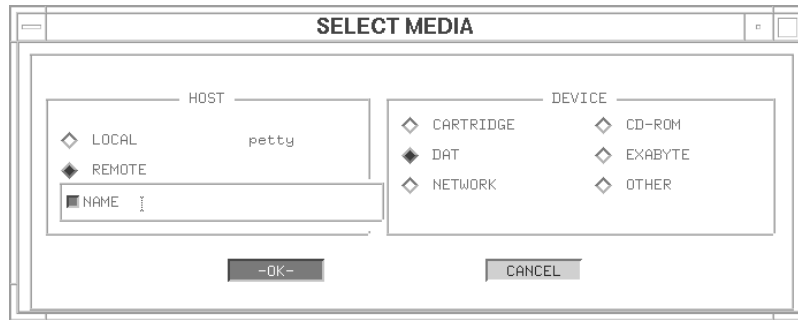


Figure 4-10 SELECT MEDIA Window

8. In the DEVICE box, select the media type (i.e., DAT or EXABYTE). If you wish to manually enter the device file, use the OTHER selection and enter the name of the no-rewind device.

Note: On Solaris, ensure you use the Berkeley device designation (e.g., `/dev/rmt/1mbn`, *not* `/dev/rmt/1mn`).

9. Of you are installing from the selected device on a remote machine, in the SELECT MEDIA window, click REMOTE. A Name field appears just below REMOTE.
10. Click the button next to the Name field to display a list of hosts available on the local network.
11. From the list of available hosts, select the hostname of the remote hosts where the tape drive is located.
12. Click OK to return to the SEGMENT INSTALLER window.
13. Click Read TOC. The items that appear in the TABLE OF CONTENTS portion of the SEGMENT INSTALLER window are the names of software segments contained on the tape.
14. From the list, select the segment you wish to install and click INSTALL. A window appears, displaying an hourglass, indicating that the system is busy installing the selected segment(s).
15. When the segment installation is complete, a warning window appears stating Selected Segment(s) Installed Successfully.
16. Click the EXIT button to dismiss this warning window.
17. To view the release notes for a segment, highlight the desired segment from the SEGMENTS CURRENTLY INSTALLED box, and click REL NOTES. The RELEASE NOTES window appears, displaying the release notes for that segment (if any).

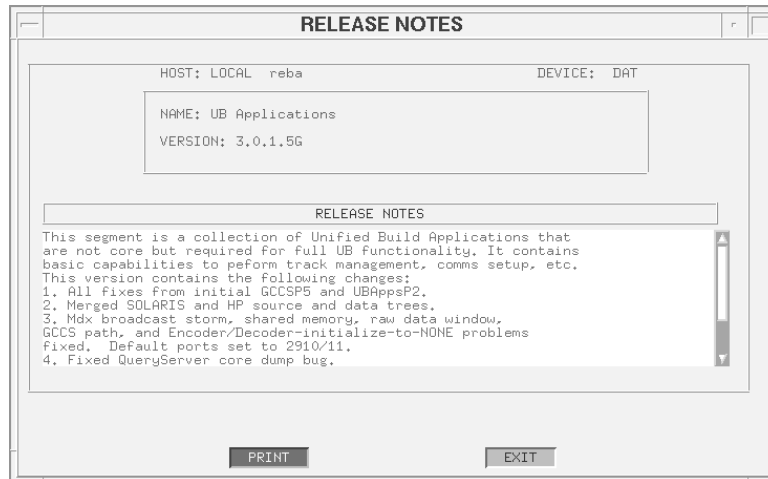


Figure 4-11 RELEASE NOTES Window

The RELEASE NOTES window displays the name of the highlighted segment, the version number, and the actual release notes.

- a. To print the contents of the RELEASE NOTES window, click PRINT.
 - b. To exit the RELEASE NOTES window and return to the SEGMENT INSTALLER window, click EXIT.
18. To remove a segment from the system, click DE-INSTALL in the DESTINATION portion of the SEGMENT INSTALLER window. (Note: The segment is removed without the appearance of a warning window.)
 19. To view the location of a segment on the disk, highlight a segment and click LOCATION in the DESTINATION portion of the SEGMENT INSTALLER window. The SEGMENT LOCATIONS window appears.

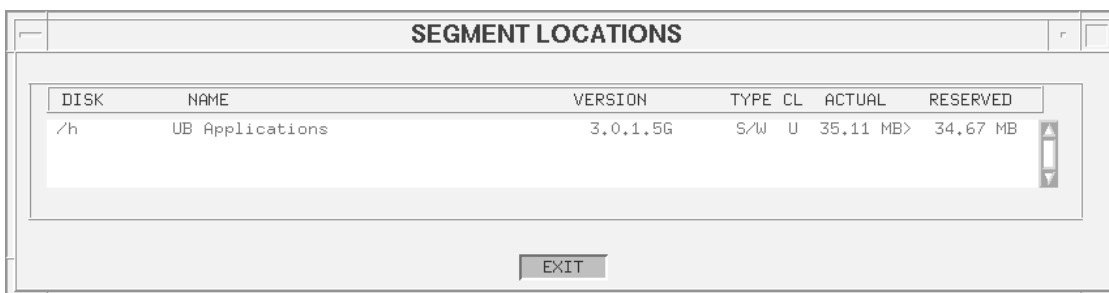


Figure 4-12 SEGMENT LOCATIONS Window

The SEGMENT LOCATIONS window tells the section of the disk where the segment is located, the type of software, the clearance of the segment, the estimated disk space needed to load the segment, and the actual disk space that was used to load the segment. Click EXIT to exit the SEGMENT LOCATIONS window and return to the SEGMENT INSTALLER window.

20. In the Segment Installer window, click EXIT to dismiss the window.

4.3.2 INSTALLATION SERVER

Use this option to "load" segments. Loading a machine "stores the software" on the machine, but *does not* enable the software to run. Each machine on the network must then be installed.

Load the software from a tape to the hard disk of one or more machines.

- A list of installation server machines is automatically created on the TDBM master.
- The list is updated each time software is loaded with this option.

Install the software using the SEGMENT INSTALLER option (described in Section 4.3.1).

To "backup" the installation server list for network installations, use the ARCHIVE NET SERVER DATA and RESTORE NET SERVER DATA options.

The INSTALLATION SERVER window is similar to the SEGMENT INSTALLER window, with the following exceptions:

- The INSTALL button is replaced by the LOAD button.
- The DE-INSTALL button is replaced by the REMOVE BUTTON.
- The SEGMENTS CURRENTLY INSTALLED list is replaced by SEGMENTS CURRENTLY LOADED ON THIS NETWORK SERVER.

4.3.3 ARCHIVE NET SERVER

The comms server maintains a list of software loaded on each machine designated as an installation server. This list is used to install software with a device specification of NETWORK. The list is updated each time new segments are loaded on network servers with the INSTALLATION SERVER option.

If the comms server goes down, a NETWORK installation is not possible because the list is inaccessible. Use ARCHIVE NET SERVER DATA on any machine that has been designated an installation server to ensure NETWORK installations will still be possible. This option copies the software list from jots1 to the machine where the option is invoked.

Note: Neither the comms server nor the designated backup comms server should be used as an installation server. If the backup comms processor has segments loaded on it, those segments will not be found when the machine is renamed because the network server list says the segments are on another system.

Also see JMCIS Installer, Installation Server, Change Machine ID (Alternate Comms Processor), and Restore Net Server Data in the Unified Build User's Guide.

4.3.4 RESTORE NET SERVER

If a backup comms processor is renamed and brought up, the list of software loaded on the network must be restored before NETWORK installations are possible. Use RESTORE NET SERVER DATA on the machine(s) where the list was copied (using ARCHIVE NET SERVER DATA) prior to the failure.

Also see JMCIS Installer, Installation Server, Change Machine ID (Alternate Comms Processor), and Archive Net Server Data in this Unified Build User's Guide.

4.3.5 ENABLE GENBROADCAST

To enable GEN Broadcast as a broadcast option for GCCS users, you must select Enable GenBroadcast from the Software menu. GEN Broadcast can *only* be enabled from the Command and Control Processor (CP) machine (typically the EM Server and TDBM Server machine).

4.3.6 DISABLE GENBROADCAST

To disable GEN Broadcast as a broadcast option for GCCS users, you must select Disable GenBroadcast from the Software menu. GEN Broadcast can *only* be disabled from the Command and Control Processor (CP) machine (typically the EM Server and TDBM Server machine). (Note: If a GCCS user has configured a broadcast as a type GEN broadcast, you will not be able to disable GEN Broadcast using this option until after you delete the existing broadcast.)

4.3.7 ADDING A NEW NIS+ CLIENT (SOLARIS ONLY)

If additional NIS+ client must be added after the installation procedure has been completed, you may modify the hosts file to add the NIS+ client machines.

1. Log in as root (default password vinson) to the NIS+ master server.

Note: NIS+ must be running in order to log in.

2. Perform the following steps to add the client to the NIS+ host table:
 - a. Enter `# cd /h/EM/nis_files` and press [Return].
 - b. Enter `vi hosts` and press [Return].

- c. Enter G and press [Return]. (This command takes you to last line of file.)
- d. Enter o and press [Return]. (This command adds a new line.)
- e. Enter <IPnumber> <CLIENT1> and press [Return].
- f. Press [Esc] and enter dd. (This command exits the insert mode and deletes the last blank line.)
- g. Enter :wq and press [Return].
- h. Enter # /usr/lib/nis/nispopulate -F hosts and press [Return].

The following text appears:

NIS+ Domainname: {DOMAINNAME}

Directory Path: (current directory)

Is this information correct? (Y or N)

- i. Enter y and press [Return].
- 3. Log in as root to the client.
 - 4. Perform the following steps to add the {NIS+ MASTER} to */etc/hosts*, if required:
 - a. Enter # vi */etc/hosts* and press [Return].
 - b. Enter G and press [Return]. (This command takes you to last line in file.)
 - c. Enter o and press [Return]. (This command adds a new line.)
 - d. Enter <IPaddress> <MASTER> and press [Return].
 - e. Press [Esc] and enter dd. Press [Return].
 - f. Enter :wq! and press [Return].
 - 5. Perform the following steps to remove any old NIS+ information (if it exists):
 - a. Enter # cp */etc/nsswitch.files* */etc/nsswitch.conf* and press [Return].
 - b. Enter # rm */etc/.rootkey* and press [Return].
 - c. Enter rm -rf */var/nis/** and press [Return].
 - d. Enter rm -rf */etc/defaultdomain* and press [Return].
 - 6. Perform the following steps to initialize the client:

- a. Enter `# /usr/lib/nis/nisclient -i -d <NIS DOMAINNAME> -h <NIS MASTER SERVER>` and press [Return]. The following text appears:

Enter server <servers name> IP address:

- b. Enter your IP address and press [Return]. The following text appears:

Please enter the network password that your administrator gave you.

- c. Enter your password and press [Return]. The following text appears:

Please enter the secman RPC password for root:

- d. Enter `nisplus` and press [Return].

Please enter the login password for root:

- e. Enter the root password and press [Return].

7. Perform the following steps to assign the client to the NIS+ domain:

Note: Ignore error messages concerning `/etc/defaultdomain`.

- a. Enter `# domainname <NIS DOMAINNAME>` and press [Return].
- b. Enter `# domainname > /etc/defaultdomain` and press [Return].
8. Perform the following steps to check the client's `/etc/nsswitch.conf` file:
 - a. Enter `cp /h/EM/systools/nsswitch.EM /etc/nsswitch.conf` and press [Return].
 - b. Enter `# cd /etc` and press [Return].
 - c. Enter `# vi nsswitch.conf` and press [Return].

Ensure the entries for `passwd`, `group`, and `hosts` look like the following:

`passwd: nisplus files`

`group: nisplus files`

`hosts: files dns nisplus [NOTFOUND=return,]`

Comment out any other lines with `passwd`, `group`, or `hosts`.

9. Perform the following steps to reboot the machine.
 - a. Enter `# cd /` and press [Return].
 - b. Enter `#`

4.4 DATABASE MENU

The Database menu provides utilities to assist in the maintenance of the databases which are created and used in GCCS/JMCIS and to provide the options for shutdown and startup of the JMCIS function within GCCS. The Database menu provides the following options:

Archive JMCIS Data

To archive current JMCIS data files to tape. (Section 4.4.1)

Restore JMCIS Data

To copy the current backup data files from tape to the JMCIS system.
(Section 4.4.2)

Clean Data Files

To delete data files from the system. (Section 4.4.3)

4.4.1 ARCHIVE JMCIS DATA

The ARCHIVE JMCIS DATA option archives current JMCIS data files to tape. You may back up some or all of the data entered into the system, such as tracks, overlays, and PIM tracks.

Warning: Be careful not to save information over important data already stored on tapes. Any tape can be overwritten during a backup if the tape is not *write protected*. To write protect a tape, open the plastic door on the back edge of the tape cartridge. Never overwrite the GCCS Operating System or JMCIS Application Software Segment tapes supplied with the system. They should be kept in a secure space so you can reinstall the software in the event of a fatal system crash.

To perform the archive, use the following procedure:

1. Insert a blank tape into the tape drive.
2. Select ARCHIVE JMCIS DATA. The tape will start to rewind. Rewinding the tape can take several minutes. When the tape is positioned, the Archive To Tape window appears.

Note: The data files displayed in the window depend on the version of software installed; your window may vary from the illustration shown below.



Figure 4-13 Archive To Tape Window

3. Click some or all of the checkboxes for the types of data to be archived. A pop-up menu is available with SELECT ALL and UNSELECT ALL options.
If you choose the ALL checkbox when creating a backup tape, the only option available when the tape is restored is ALL. However, if you select all the data files by clicking the individual checkboxes (or using the pop-up SELECT ALL), you will later be able to “pick and choose” which data files to restore.
4. Click OK to begin the backup process. When the process is complete, the tape is automatically rewound.
5. Remove the tape. Place a label on the tape and write JMCIS DATA BACKUP, with the date, version, and classification. Check with the designated authority for classification level required.

4.4.2 RESTORE JMCIS DATA

The RESTORE JMCIS DATA option copies the current backup data files from tape to the JMCIS system. This backup tape must be one created using the ARCHIVE JMCIS DATA option.

Warning: Track data, message logs, and AEN table information must be restored to the comms processor. Restoring these types of data to any other machine while the comms processor is running could cause serious problems. However, other data types, such as overlays or PIM tracks, can be restored to any machine on the LAN.

Restored data is not merged with existing data. Existing data is completely replaced by the data on the tape.

To restore data files:

1. Insert the data file backup tape into tape drive.
2. Select RESTORE JMCIS DATA. A Restore From Tape window similar to the figure below appears.

Note: The data files displayed in the window depend on the version of software installed; your window may vary from the illustration shown below.



Figure 4-14 Restore From Tape Window

The Restore From Tape window displays the DTG stamp made at the time the data was backed up. Only those types of data stored on the tape appear as choices in the window.

3. Click any or all of the checkboxes for the types of data to restore to the system from the backup tape. A pop-up menu is available with SELECT ALL and UNSELECT ALL options.
4. Click OK to begin the restore process.

When the restore process is complete, the tape rewinds automatically.

4.4.3 CLEAN DATA FILES

The CLEAN DATA FILES option enables you to delete datafiles from the system. Different groups of datafiles can be deleted, including all existing track information. This option is used mainly to clear bad message data from the message logs. This option is also very useful if the display seems corrupted. Cleaning the local MAP TOGGLES will often correct this problem.

To clean data files:

1. From the DATABASE menu, select CLEAN DATA FILES. The CLEAN DATA FILES window appears.

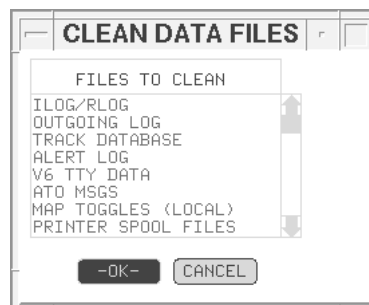


Figure 4-15 CLEAN DATA FILES Window

The CLEAN DATA FILES window displays a list of files that may be erased.

2. Select the files you want from the list and click OK to erase those files. (To close the window without erasing any files, click CANCEL.)

After cleaning the data files, those files that have been erased will no longer appear in the system. For example, if you erased the TRACK DATABASE files, all of the tracks will be removed from the tactical display (except OWNSHIP) when the system is started again. Selecting PRINTER SPOOL FILES removes all print requests queued in the system.

4.5 NETWORK MENU

The Network menu provides utilities to manage the general configuration of individual workstations as well as the local LAN and to manage the interface between the workstations and the LAN. The Network menu provides the following options:

Change Machine ID

To change the name of a machine on a network. (Section 4.5.1)

Set System Time

To set the time on the workstation to match that of the comms server. (Section 4.5.2)

Set WAN UID

To set the wide-area network (WAN) unique ID (UID). (Section 4.5.3)

Set WAN DDN Timeout

To allow the system administrator to set a time-out period for DDN network operations. (Section 4.5.4)

Config DDN Host Table

To create a Data Defense Network (DDN) host table to describe the entire WAN. (Section 4.5.5)

System Configuration

To set the list of available hosts for the local machine. (Section 4.5.6)

4.5.1 CHANGE MACHINE ID

The CHANGE MACHINE UNIQUE ID option changes the name of a machine on a network.

WARNING: The machine will reboot when you use this utility. If circumstances prevent you from rebooting the machine, do not use this option.

Each workstation on an Ethernet must have its own unique network address. This address is set when the system is installed and is associated with a symbolic name. The network does not permit two machines with the same name. Select CHANGE MACHINE UNIQUE ID to view the Change Machine ID window:

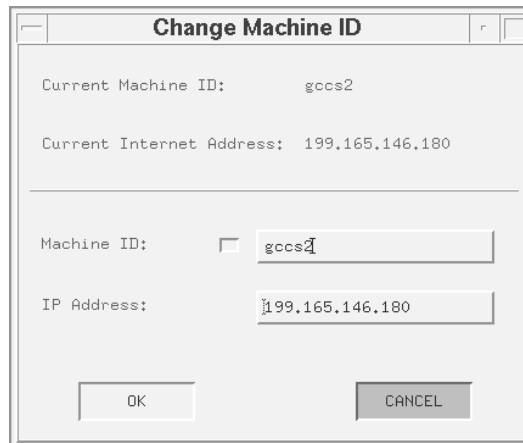


Figure 4-16 Change Machine ID Window

1. Click the up or down arrow to scroll through the list of machine names.
2. After selecting the machine name, click OK to complete the change. (If the name is already used on the LAN, an error message prompts for another name.)
3. After the name is accepted, a warning window alerts you that the system will reboot.
4. Click OK to reboot the machine or CANCEL to prevent the reboot. The reboot is required to change the name (ID) of the machine.
5. After the reboot process is complete, you are returned to the Login window.

4.5.2 SET SYSTEM TIME

The JMCIS comms processor must have the correct ZULU time or track reports may fail to process. JMCIS will not process track reports “in the future” (i.e., with time/pos lines ahead of the JMCIS clock). To avoid failed track reports, set the JMCIS system time as follows:

1. From the NETWORK menu, select the SET SYSTEM TIME option. The SYSTEM TIME window appears.

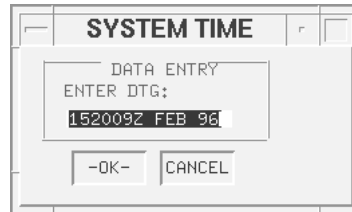


Figure 4-17 SYSTEM TIME Window

2. Enter the correct ZULU time in DDHHMMZ MON YR format.
3. Click OK to set the JMCIS system time.

4.5.3 SET WAN UID

A unique ID (UID) is critical to the integrity of the Data Defense Network's (DDN) contact database. Each wide-area network (WAN) site is assigned a unique address. This address and the corresponding unique name of each system on the network are used by the system to create a UID for each contact that enters the system. Note that the UID is displayed in the track edit window in a non-edit field, and therefore it cannot be altered by the operator.

The UID is formatted as XXX, where XXX is a three character WAN DDN UID, or station identifier, assigned to your particular JMCIS system. The three-character ID marks tracks added to the DDN from your system.

The UID code you provide using this window ensures that tracks added to the database from two different terminals on the WAN are uniquely identified *even if they are added at precisely the same time*. While the time/date stamps of the two tracks may be identical, the first three characters of the UID are different since the contacts were added at different stations. Thus, the two parts of the UID work in conjunction to uniquely identify every track added to the track database.

Each track is assigned a UID. However, the UID may or may not be used depending on your system's operating mode. For example, if UID CORRELATION MODE is selected in the EDIT FOTC CONFIGURATION window, any contact database information received over the DDN is processed according to its WAN DDN UID before any other type of correlation is done. This first pass through the database looks solely for exact UID matches to the incoming track. UID matches are updated directly regardless of any other considerations such as attribute mismatches or geofeasibility concerns. The track's history is updated and, in the event of mismatched attribute data, existing attribute information is replaced by that of the

incoming track. If no match is found in the track database, normal attribute correlation is then performed.

In general, ashore installations operate in FOTC Non-participant or in UID Correlation mode, while afloat sites select from FOTC Coordinator, FOTC Participant, or FOTC Non-participant modes.

Warning: For Ashore Sites Only

Using UID Correlation mode without a valid WAN DDN UID can cause serious database problems. Do not select UID Correlation mode before you have entered a valid WAN DDN UID.

From the NETWORK menu, select the SET WAN DDN UID option to set your system's WAN DDN UID. The SET WAN UID window appears.

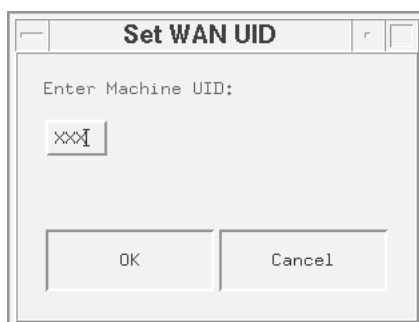


Figure 4-18 Set WAN UID Window

Enter your assigned UID into the highlighted field, then press [Return]. (Or, if you prefer, enter the UID and click OK.) If you decide not to change the default UID, click CANCEL.

4.5.4 SET WAN DDN TIMEOUT

This option allows the system administrator to set a timeout period for DDN network operations. The timeout period begins after the DDN channel is started.

If a requested connection to a remote host fails, or if the receipt timeout period expires, a DDN STATUS UNCERTAIN warning is put in the alert log. (If the DDN TIMEOUT knob in the SCREEN ALERT FILTER window is selected, a window also appears on the tactical display.)

Select the SET WAN DDN TIMEOUT INTERVAL option to set your system timeout. The DDN TIMEOUT window appears:

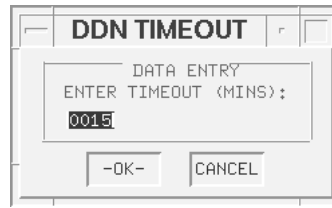


Figure 4-19 DDN TIMEOUT Window

Timeout values must be between 1 and 3600 minutes. The default value is 15 minutes (0015). Enter the desired timeout length (in minutes) into the highlighted field, and click OK. If you decide not to change the default value, click CANCEL.

4.5.5 CONFIG DDN HOST TABLE

Warning: This option is for use only by hub sites.

If you are a hub site and you need to reload the JMCIS software for any reason, make sure to restore the data for this option using your tape backup of the DDN host table after the basic installation has been completed. If you do not have a tape backup of the DDN host table, follow the steps listed below to recreate the DDN host table.

The Data Defense Network (DDN) host table describes the entire wide-area network (WAN). A “generic” host table is established in the operating system during installation. The system administrator must edit a copy of the generic table so that each site with which you intend to communicate given a UHID. Most sites communicate with only a few other sites, so unedited host table entries should be deleted.

Note: Sometimes a site is designated to be a backup for a centralized communications site. The backup site must be prepared to quickly go on-line in case the system at the primary site, or hub, goes down. The CONFIGURE DDN HOST TABLE option provides a means to store two separate host tables, allowing you to quickly go on-line as a hub. If your site serves as a backup communications hub, you should set up the two host tables as follows:

- Primary: lists the sites you need for normal communications.
- Alternate: lists the sites used by the hub that you are backing up.

The easiest way to configure these tables is to set up the alternate table *first*, then set up the primary table, which is usually a subset of the sites listed in the alternate table.

Once the tables have been set up, it is easy to switch between the two. The current table appears as part of the NET HOSTNAME TABLE window title. If the window title reads NET HOSTNAME TABLE–ALTERNATE, select PRIMARY from the window's pop-up menu to view the sites you use under normal operating circumstances. If the window title reads NET HOSTNAME TABLE–PRIMARY, select ALTERNATE from the window's pop-up menu to see the entries used by the hub you are backing up.

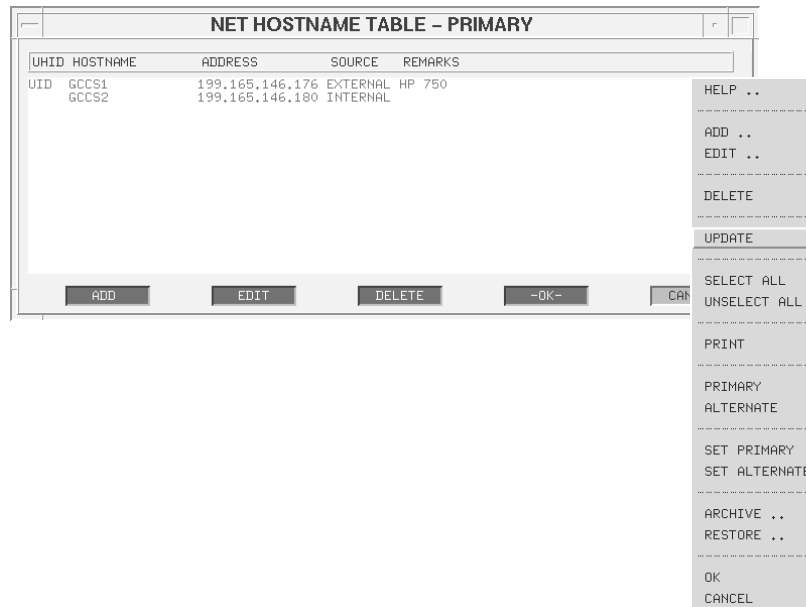


Figure 4-20 NET HOSTNAME TABLE– PRIMARY Window, with pop-up menu

The following steps describe how to set up the DDN host table.

1. Select CONFIGURE DDN HOST TABLE from the SYSTEM ADMINISTRATION window.
2. Select UPDATE from the pop-up window to read a copy of the host table from the operating system. The entire file is read in from the operating system.
3. If your site serves as backup for a hub site, select SET ALTERNATE from the pop-up menu. *If your site is not a hub backup, skip to Step 4.*
4. Select the first site in the default list with which you will routinely communicate.
5. Click EDIT to bring up the EDIT HOSTNAME window. Fill in the site's UHID, hostname, address, and any desired remarks in the appropriate fields.

6. Note that the default for each site is *internal*. If the site is external, make sure to click the checkbox so it appears empty. An empty checkbox means that the site is *external*.
7. Click OK.
8. Repeat Step 4 through Step 7 for each of the remaining sites with which you communicate.
9. Choose the SELECT ALL option from the pop-up menu.
10. Deselect all the sites you just edited; they appear at the top of the list.
11. Click DELETE to remove all the highlighted sites since they have not been assigned a UID.

Note: Perform Step 12 through Step 15 only if your site is a hub backup. Otherwise, skip to Step 16.

12. Select SET PRIMARY from the CONFIGURE DDN HOST TABLE window pop-up menu.
13. Highlight and delete any sites that you will not communicate with under normal operating conditions.
14. If you need to add any sites to the primary list, click ADD. Enter the site's UHID, hostname, address, and any desired remarks in the appropriate fields. If the site is external, make sure to click the checkbox so it appears empty.
15. When the list contains all sites you will communicate with under normal operating conditions, select SET PRIMARY from the pop-up menu.
16. Archive the host table to the clipboard, then make a tape backup of the host table data. *If your site serves as a hub backup, make tape backups of both the primary and alternate host tables.* Store the backup tape in a safe place so that you can recover quickly in the event your host tables become corrupted.

DDN, in general:

- Click ADD to add a new site to the DDN hostname table.
- Click EDIT to edit the UHID, hostname, address, remarks, or internal/external flag of an existing site.
- Click DELETE to remove an existing site from the list.
- Click CANCEL to close the NET HOSTNAME TABLE window without saving your changes.
- Click OK to store the new configuration.

4.5.6 SYSTEM CONFIGURATION

In order for a local workstation running GCCS software to be fully operational within the LAN, a list of hosts in the LAN must be configured on the local machine. The SysCon window provides an interface to set the host names in the resource files that are required to run GCCS software.

To view the current SysCon window, select System Configuration from the Network menu. The SysCon window appears.



Figure 4-21 SysCon Window

Two types of hosts may be set using the SysCon window: Full hosts and Printer hosts. Full hosts are other hosts on the network, including the administrative, broadcast, and pcm hosts. Printer hosts are print servers or printer clients for the various printers that may be enabled from the workstation. A Full host may also be used as a printer server. The Full hosts defined in this function are provided as hosts for various functions in GCCS, including available MACHINE options on various communications interfaces.

The SysCon window initially displays a generic listing of 30 potential full hosts and 5 printer hosts in a Hosts box on one side of the window (defaults to jots1 through jots30 and milan 1 through milan 5). Note that the first entry in this list of hosts is non-editable and reflects your workstation's TDBM Master entry, set by entering the TDBM Master hostname in the TDBM Master field to the right of the Hosts box.

To the right of the Hosts box in the SysCon window, several fields allow you to define specific hosts which provide specific services and networking functions in conjunction with your workstation. The Local Hostname field is a non-editable field that displays your workstation's hostname. The TDBM Master: field allows you to set the TDBM Master hostname. This field also determines the setting for the Full Host #1 in the Hosts box. Several other field allow you to define other server hosts (broadcast, pcm, etc.) related to the workstation.

Note: On GCCS networks, the 5 printer host (milan) fields should always be left empty.

To set the hosts available to the workstation:

1. In the Hosts box on the left side of the SysCon window, click the toggle box beside the host entry you wish to change. Note that when the toggle box is activated (yellow), the host is designated as a Full host; and when the toggle box is deactivated (empty), it is designated as a Printer host (and the label name changes from Full Host to Printer Host).
2. Click the name field next to the appropriate toggle box. The field will become active and is now editable. Enter the name of the host.

Note: The TDBM Master host is entered as Full Host #1. Any other hosts on the local network should be entered as subsequent hosts (Full Host #2 through Full Host # X).

3. Click OK to save the changes you have made to the Hosts box.

Note: Whenever OK is clicked, the SysCon window saves the changes made up to this point and closes. In order to further edit the window, you must restart the window from the Network menu. If you choose, you may make multiple changes to the window per session without clicking OK.

To delete a host entry:

1. Select the host to be deleted and clear the corresponding host name field.
2. Click OK. The SysCon window closes, saving the changes. Because the system will not maintain an “empty” host entry, when you reopen the SysCon window, the entry that was left empty will be eliminated from the system.

The Hosts box displays the list of hosts that are available on the LAN. A total of 30 Full host entries are available, but more may be added, if required.

To add a host entry:

1. In the Hosts box, click NEW. A new entry appears at the bottom of the scroll box.
2. Set the new host as described previously in this section.

Note: When the 31st (or later) Full host is added to the list displayed in the Hosts box and OK is clicked, a warning window appears, informing you that the system may not recognize more than 30 full hosts. This limitation is based upon your local machine's capabilities. If your machine is capable of supporting additional hosts, then clicking SAVE ANYWAY in the warning window saves the additional host(s) and dismisses the warning window. If your machine is not capable of supporting

the additional host(s), clicking FIX IT NOW returns you to the SysCon window, where you may modify the host listing to comply with the machine limitation.

When all necessary hosts have been defined in the Hosts box, you must define which hosts serve specific network/server functions on the LAN.

To assign specific host roles:

1. Verify the hostname in the Local Hostname: field. This should be your workstation's hostname.
2. In the TDBM Master: field, enter the TDBM Server hostname for your workstation.
3. Enter the appropriate hostname in the following fields:

admin	qs
prt	wdbm

Note: Typically, in the GCCS environment, both the TDBM server and TDBM clients should have the TDBM server hostname in each of the above fields. However, to account for diverse configuration capabilities, any hostname may be entered in these fields.

4. Click OK to save the changes you have made to this portion of the window and dismiss the SysCon window.

Notes

Notes

CHAPTER 5: COMMUNICATIONS

5.1 THE JMCIS NETWORK

A TAC-3/4, Sparc 10/20, or RSC Gray Box loaded with the JMCIS software can be a standalone machine or networked in a server-client relationship.

Standalone

A standalone machine is its own server. It retains data without relying on a networked server. It shares data through messages transmitted over configured comms ports, or by floppy disk or tape.

Network

The communications processor (often called the CP, server, or jots1) holds all track and comms data. When installing software, the CP should be installed first, followed by its client machines. Client machines are dependent on the server for data, especially data from the track database. CP functions include:

- Processing incoming and outgoing messages.
- Decoding incoming messages.
- Correlating track information.
- Routing outgoing messages.

If the server goes down, the Track Database Manager (Tdbm) warning window informs the user that the server is down. Though the user can view track information, no track database actions (local or shared) are processed.

Workstations running different versions of JMCIS software (2.1.2.1 and above) can exchange track data using:

- GENBROADCAST segment
- MDX interface (described in *Comms* chapter of the *UB User's Guide*)

5.2 INTERFACE DESCRIPTION

JMCIS supports two interface types— serial and LAN.

5.2.1 SERIAL INTERFACE: RS-232, RS 422, MIL-188

Used for serial communication between JMCIS and another system (such as POST).

- If at the same site, connect them directly.
- If at different sites, connect them through a secure modem, such as a STU III.

Refer to *C3 MIL-188/RS-422/RS-232 Interface Converter Technical Description*, C3 Incorporated, Herndon, Virginia, for DIP switch settings for each interface.

5.2.2 LAN INTERFACE: ETHERNET AND FIBER OPTIC CABLING

Used for communications between two or more JMCIS workstations on a LAN.

- Each machine is assigned a unique name and address on the network.
- These are used by system files.

5.2.3 PROTOCOLS

TCP/IP

Transmission Control Protocol (TCP) moves data in a continuous, unstructured byte stream. It provides full-duplex service, acknowledgment of data received, and data flow control.

Internet Protocol (IP) provides network layer services to the TCP/IP protocol suite. IP is responsible for forwarding packets through a network based on IP addresses. IP relies on TCP to guarantee delivery of packets.

X.25

Used for a Wide Area Network (WAN) of computers connected by a Packet Switching Network (PSN), such as the Defense Data Network "DSNET1." (Generally used by ashore sites only.)

5.3 PHYSICAL CONNECTIONS

5.3.1 SERIAL

Requirements for a Direct Connection

A 2-, 3-, and 7-pin connection is required to connect JMCIS and other systems, such

as POST, located in the same installation.

Requirements for STU III Connection

The STU III must support an RS-232 connection. If not, request an RS-449-to-RS-232 adapter from the manufacturer.

A TAC-3/4 requires:

- A DB 9 female-to-DB 25 male cable.
- Certain models of STU III require voltage on pins 4 and 20, which the TAC-3/4 does not supply. A special adapter must be used.

An RSC Gray Box requires:

- A DB 25 male-to-male cable.

5.3.2 LAN

Requirements for an Ethernet Connection

- Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.
- The copper LAN interface may have a BNC connection between transceivers.
- The network must be terminated at both ends.
 - Use a terminating 50 Ω resistor on each end.
- If the workstation is a standalone configuration, the LAN connections on the workstation must be terminated.
 - Use a 50 Ω resistor on each.

Requirements for a Fiber Optic Connection

- Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver (Fibercom box).
- Fibercom boxes (nodes) must reside at each computer connected by fiber optics.

These boxes have dual-ring capability to ensure continued transmission.

For example, if a transmission is interrupted by a broken fiber optic or connection, it is automatically routed to the second ring.

5.3.3 X.25

Requirements for an X.25 Connection (TAC-3/4)

- If the system is configured for DDN communications, the Serial A port must be the DDN/X.25 interface device. No other device may be configured to the TTYA port.
- A DB 15 connects the machine to a modem and encryption device with an X.25 interface.
- The X.25 card provides synchronous RS-232 (DTE) error-free transmission over the PSN.
- There may be many interfaces, such as crypto, modem, or leased line, between the computer and the actual PSN.

5.4 COMMUNICATION AND BROADCAST CONFIGURATION

To configure a communications channel, use the COMMUNICATIONS option (described in the *UB User's Guide, Comms* chapter.)

Modify fields to configure the channel. Keep in mind the following general information:

- It is best to use standard comms settings— changing some settings, such as baud rate, parity, or stop bits, could cause data to be garbled.

For example, if messages are garbled, it's likely that the transmitting and receiving sites don't have the same values set for the baud rate and related fields.

- XON/XOFF should never be used for baudot data connections.

Toggle on the XON/XOFF checkbox support the use of the XON/XOFF commands to stop and resume transmission.

- If the RTS/CTS checkbox is toggled on, a Request to Send (RTS) message will be sent before the real message is sent.

The recipient will reply with a Clear to Send (CTS) message when it's prepared to receive the data.

These channels are installed as the master default list of comms channels.

<i>TTY DEVICE</i>	<i>ASSIGNED TO</i>
A	Printer
B	TRE/TRETABULAR
C	GFCP/Terminal Control
C0	Link-11 (PED, PIH)
C1	OTCIXS-TTY
C2	OTCIXS
C3	TADIXS
C4	Ownship NAV Interface
C5	Link-14
C6	HIT-BCST
C7	FLT-BCST-1
D	GENSERPOST
D0	(none)
D1	TADIXS TTY
D2	DTC
D3	Remote Link-11 (future)
D4	Remote Link-11 RXA (future)
D5	Remote Link-11 RXB (future)
D6	FLT-BCST-2
D7	(none)
NTDS0	ACDS Link-16 (optional) 2-way Link-11 WRN-6 WSN-5 SDMS

Important:

- Device A is not assigned to a comms channel. It is assigned to the printer.
- C_n and D_n channel assignments are valid only when 8-port MUX boards are used.
- NTDS_n channel assignments are valid only when NTDS boards are used.

If settings have been modified (device settings, protocol parameters, or both) it is possible to return to the original system defaults, but pay attention to the following:

- Information pertaining to any new channels is removed. The current list can be saved to recall later.

- To save the current settings:
 1. Select DEFAULTS from the COMMUNICATIONS window pop-up menu to open the DEFAULTS window.
 2. Enter a name in the SAVED NAME field and click SET.
- To recall these settings:
 1. Open the DEFAULTS window.
 2. Highlight the name assigned to the saved settings and click GET.
 3. The system stops and restarts all channels.
- To reset channels to the original system defaults, select MASTER DEFAULT from the COMMUNICATIONS window pop-up menu.

The system stops and restarts all channels.

Remember, incoming messages could be lost during the time it takes to accomplish this task (approximately 1–2 minutes).

5.4.1 STARTING COMMS CHANNELS

A comms channel must be turned on before it can be used. Comms channels are turned on and off with the COMMUNICATIONS option from the COMMS pull-down menu.

COMMUNICATIONS							
NAME	XRF	INT	INTERFACE	MACHINE	DEVICE	STARTUP	STATUS
LINK11-IH	LIH	EXT	LINK11IH	JOTS1	TTYC0	AUTO	ON
LINK11-EDO	LED	EXT	LINK11EDO	JOTS1	TTYC0	MANUAL	OFF
OTCIXS	OTC	EXT	OTCIXS	JOTS1	TTYB	AUTO	ON
DTC	DTC	EXT	SERIAL	JOTS1	TTYC2	AUTO	ON

ADD EDIT DELETE EXIT

Figure 5-1 Communications Window

Channels are turned on and off one of two ways:

- Highlight the channel; select START, STOP, or RESTART from the pop-up menu.

- Toggle the AUTOSTART checkbox ON, in the COMMS EDIT window. This turns a channel ON at system startup.

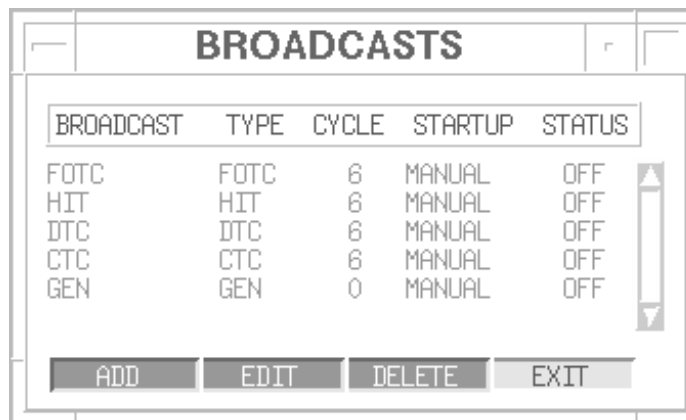
The STATUS column indicates status of each channel: ON or OFF.

Important:

- A comms channel can only be turned on if the designated device exists.
For example, the DTC comms channel in Figure 5-1 is assigned to TTYC2. If a multiplexer is not connected to the TTYC port, this channel can't be turned on, but it can be reassigned to an existing port.
- A channel must be ON to open its status window.
Highlight the channel.
Select the WINDOW pop-up option.

5.4.2 STARTING BROADCASTS

A broadcast must be turned on before it can be used. Broadcasts are turned on and off using the BROADCASTS option from the FOTC/BCST menu. The BROADCASTS window displays a list of available broadcasts.



BROADCAST	TYPE	CYCLE	STARTUP	STATUS
FOTC	FOTC	6	MANUAL	OFF
HIT	HIT	6	MANUAL	OFF
ITC	ITC	6	MANUAL	OFF
CTC	CTC	6	MANUAL	OFF
GEN	GEN	0	MANUAL	OFF

ADD EDIT DELETE EXIT

Figure 5-2 Broadcasts Window

Broadcasts are turned on and off one of two ways:

- Highlight the broadcast; select START from the pop-up menu.
- Toggle the AUTOSTART checkbox ON in the BROADCAST EDIT window. This turns the broadcast at system startup.

The STATUS column indicates status of each broadcast: ON or OFF.

5.4.3 MESSAGE TRANSMISSION

Messages are sent manually (using an XMIT option) and automatically (using a broadcast).

To transmit, make sure:

- The communications channel is turned on.
- The channel is configured properly.
- The channel can transmit messages.

Note: Manual transmissions are not allowed on the DTC channel; only automatic transmissions via the DTC broadcast.

To broadcast, make sure:

- The appropriate comms channels are running, as described in the previous section.
- The appropriate broadcast programs are running, as described below.

5.4.4 MESSAGE AND BROADCAST HEADERS

To set a default message header for manual transmissions, click DEFAULT in the HEADER EDIT window pop-up menu. This header is used for all options with a manual transmit capability, such as tracks and overlays.

Each broadcast has its own header. If DEFAULT is selected while creating a header for a broadcast, the broadcast header becomes the default message header. This header is used for manual transmissions *and* for the broadcast.

5.5 STU III CONFIGURATION

Keep in mind the following information when configuring a STU III.

- A serial interface comms channel must first be configured for the STU III connection (see also *Physical Connections*):
 - Set the device to the port connected to the STU III.
 - Use serial interface defaults for the other settings: data type=ASCII, parity=NONE, stop bit=1, baud rate=2400, data size=8, RECV and XMIT=ON.
- An entry must be made in the Auto-Forward Table. (See *Auto-Forward Table* in the *Unified Build User's Guide*.)

- An entry must be made in the Sources reference table if in FOTC mode. (See *Source XREF Table* in the *Unified Build User's Guide*.)
- Both STU IIIs must be in Remote Control Mode with Secure Access Control System (SACS) enabled.
- Both STU IIIs must have proper ACLs loaded.
- STU IIIs with SACS support auto-answer auto-secure— no operators are needed. In this mode, Voice/Secure Voice options are unavailable.
 - SACS grants access to designated STU IIIs, as identified in the ACL on the local STU III.
 - Three requirements for secure authentication of automatic, incoming calls are: ACL header, DAO code, and Keyset ID.
 - STU IIIs (including STU III SACS) without these codes are excluded, and cannot gain access or connect with STU-IIIs that share DAO codes or keyset IDs.
 - This creates a closed network. Unauthorized calls are disconnected before the line to JMCIS is opened.
- If two STU IIIs can talk to each other, but can't transmit data, their internal modes may be different. Check baud rates: synchronous and asynchronous must match.

5.5.1 PROCEDURES

Download ACL

The following tables illustrate the sequence of a JMCIS ACL download. This sequence has been tested on AT&T devices only.

1. Insert the Master CIK.
2. Press MENU.

<i>OBSERVE</i>	<i>PRESS</i>
Main Menu Secure Voice	NEXT
Main Menu Secure Data	NEXT
Main Menu Show Config	NEXT
Main Menu Change Config	SELECT
Change Config Security Config	SELECT
Security Config SACS Disable	NEXT
Security Config SACS Options	SELECT
SACS Options SACS Control	NEXT
SACS Options Auto Access Control	NEXT

SACS Options Far-end ID	NEXT
SACS Options Access List	SELECT
ACCESS LIST MENU Load ACL Via DTE	SELECT
WAITING FOR ACL start DTE transfer	(begin download)
RECEIVING ACL please wait	(wait until finished)
ACL RECEIVED nnn show new ACL	NEXT
ACL RECEIVED nnn save new ACL	SELECT
NEW ACL SAVED previous menu	MENU

Temporarily disabling SACS ACL

1. Insert the Master CIK.
2. Press MENU.

<i>OBSERVE</i>	<i>PRESS</i>
Main Menu Secure Voice	NEXT
Main Menu Secure Data	NEXT
Main Menu Show Config	NEXT
Main Menu Change Config	SELECT
Change Config Security Config	SELECT
Security Config SACS Disable	SELECT
SACS Disable on/off change Disable	SELECT

Autodialing Between Two AT&T STU IIIs

1. Insert the Master CIK.
2. Press MENU to turn auto-answer on.
 - After the ACL is downloaded, but *before* it is put in Remote Control Mode, auto-answer must be on.
 - If the display indicates one or more AASD rings, auto-answer is on.

<i>PRESS</i>	<i>PRESS</i>
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
NEXT until "SAC Options"	SELECT
NEXT until "SACS Control" (Ensure SASCTRL is enabled.)	SELECT

<i>PRESS</i>	<i>PRESS</i>
MENU	MENU (again)
NEXT until "Change Config"	SELECT

NEXT until "Security Config"	SELECT
The display panel will read SACS Disable (Ensure SACS Disable is OFF.)	SELECT

<i>PRESS</i>	<i>BUTTON</i>
MENU	MENU (again)
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
NEXT until "SACS Options"	SELECT
NEXT until "Auto Access Ctrl"	(Ensure Auto Access Ctrl is ON.)

<i>PRESS</i>	<i>BUTTON</i>
MENU	MENU (again)
NEXT until "Change Config"	SELECT
NEXT until "Auto-Answer"	SELECT

5.5.2 CONFIGURING SPECIFIC STU-III MODELS

Motorola SECTEL 1000/2000:

- This device provides the auto-secure feature, but does not allow auto-answer, nor does it support SACS.
- The default data mode is 2400 baud, asynchronous.
- An RS-232 port is included, allowing direct connection to JMCIS.
- A serial communications interface must be used.

RCA STU III:

- The STU III data port is an RS-232 (DB 25) or an RS-449 (DB 37) connection, depending on manufacturer and model.
- RS-232 and RS-449 share the same signal levels but have a different pinout.
- RS-449 ports must be converted to RS-232 to work with JMCIS. These converters are included with the STU III.

The following table illustrates the conversion requirements of a STU III RS-449 configuration to an RS-232.

RS-449 (STU-III)	RS-232 (TDP)
------------------	--------------

1-Shield	1-Shield
4-Send Data (+)	2-TXD
6-Receive Data	3-RXD
7-Request to Send	4-RTS
9-Clear to Send	5-CTS
11-Data Mode	6-DSR
19-Common Return	7-Common
20-Receive Common	
22-Send Data (-)	
37-Send Common	
12-Terminal Ready	20-DTR

To configure an RCA STU III:

1. Press PROGRAM.
2. Press SETUP.
3. Press YES at “set terminal options.”
4. Press YES at “set standard options.” The standard settings are:
 - Dialing mode: TONE
 - Comm mode: FULL DUPLEX
 - Data Ports: 2400 ASYNC
 - Remote Capable: DISABLED
 - A-lead Control: ENABLED
 - Dual Home: Line 1 only

5.6 TROUBLESHOOTING COMMUNICATIONS PROBLEMS

If messages are not being received or transmitted, the problem may be solved by checking the following hardware and software components. Correcting every communications problem is beyond the scope of this document, however some common trouble areas include:

- Connections between communications hardware and the workstation running JMCIS are established incorrectly.
- External communications devices are set incorrectly.
- Options that affect communications within JMCIS are set incorrectly.

NOTE: Within this section, “COMMS MENU” refers to the menu on the JMCIS screen, *not* the System Administrator screen.

5.6.1 HARDWARE PROBLEMS

Check the following:

- Communications antennas must be positioned to the proper azimuth.
- Radios must be up and running, with everything set correctly.
- Modems must be running properly.
- Cryptologic devices must be loaded and set correctly.
- Devices connected to JMCIS (for example, the (V)6) must be operational and set correctly.
- Connections must be tight.
- Check data converters.
- If the connection is serial, test the line with a breakout box.
 - Connect the breakout box to the machine, then to the comms line.
 - Verify signals are being provided by both sides without conflict. For example, the machine and the comms line could both have a signal on pin 2.
- If a properly configured comms channel is connected directly to a crypto/radio, and data results, check for an improper crypto hardware or crypto key.

5.6.2 SOFTWARE PROBLEMS

Check the following:

- Comms channels must be running. Otherwise, incoming messages could be lost and outgoing message could overload the buffer.
- Use incoming message logs and outgoing message logs to verify that messages are entering and leaving the system.

Messages that have not been transmitted display as dots in the MSG TOT field (outgoing message logs).
- Comms channel parameters must be set correctly.
 - The machine associated with the comms channel in JMCIS must be the same machine to which the channel is connected.
 - The port (device) listed for the comms channel must be the same port to which it is connected.
- If messages are garbled, check the comms channel parameters such as baud rate, stop bits, etc.

- If messages are received but tracks are not displayed, check:
 - INPUT MSG FILTERS
 - INPUT GEO FILTERS
 - FOTC PARAMETERS (FOTC/BCST menu)
 - Applicable options in the PLOT CONTROL menu
- If the channel is a serial interface, toggle on the CRYPTO PHASE checkbox to make sure messages are handled properly.

This checkbox is available for systems using the KG-84 encryption device (usually operating at 75 baud).

5.6.3 SPECIFIC CHANNELS AND INTERFACES

Troubleshooting suggestions for the following channels are addressed in this section:

- OTCIXS (including (V)6 and message backlog)
- OTCIXS-TTY
- Link-11
- DTC
- Low Data Rate(LDR)
 - HIT-BCST
 - Link-14
- Ownship/Navigation
- MDX

OTCIXS

To check the status of the OTCIXS channel, or to correct communications problems, follow these steps until the problem is solved. While troubleshooting an OTCIXS problem, *turn off the OTCIXS broadcast to prevent a message backlog!*

1. Review the information in the OTCIXS STATUS window.
 - Select COMMUNICATIONS from the COMMS menu.
 - Highlight the OTCIXS channel.
 - Select WINDOW from the pop-up menu to access the OTCIXS STATUS window.
2. Troubleshoot the JMCIS (V)6 interface (described below in *JMCIS (V)6* and

Message Backlog).

3. Check that the General Front-end Comms Processor (GFCP) is turned on and functioning properly, if necessary.

JMCIS/(V)6

If the INTERFACE STATE field in the OTCIXS STATUS window reads DOWN, check the (V)6 to see if it's online. If so, initialize it again to reestablish the "handshaking" interface.

If the INTERFACE STATE field does not read DOWN, but messages are not being received or sent, follow these steps until the problem is corrected:

1. Check the NET field. It should display OTCIXS/TADIXS.
 - If it reads FLTSAT VOICE 1 or 2, then the (V)6 is set incorrectly.
 - Correct the (V)6 settings, then reinitialize.
2. Check the NET STATUS field to see if it reads NO NET CONTROL. This indicates one of four problems:
 - radio
 - satellite antenna
 - crypto
 - loose connection
3. Run a Satellite Loop (SAT Loop) Test on the (V)6. If this test fails, it means the (V)6 is not communicating with the satellite.
 - Check the communication paths, frequency, W3 status, and the position of the satellite antenna.
 - SAT Loop may fail several times if the net is busy.
4. Run a Crypto Loop Test on the (V)6. If this test fails, check the encrypting device to see if it needs reloading.

This test does not validate “correct” crypto keylist or keylist day.
5. Stop the OTCIXS comms channel.
6. Restart the OTCIXS comms channel.
7. Reinitialize the (V)6.

Message Backlog

The (V)6 queue holds a maximum of 50 messages. When the queue is full, an alert notifies the user, but only if alerts have been turned on. (See the *Unified Build User's Guide* for information on setting alerts.) An alert usually indicates that a hardware problem is causing the backlog.

Remember: If the (V)6 buffer is full, messages can backlog in the JMCIS outgoing queue even though there is no problem between JMCIS and the (V)6.

Check the following:

- Confirm the backlog in the OUTGOING MESSAGE LOG window.
 - Messages not sent to the (V)6 from JMCIS appear as dots in V6# field.

- Messages sent from JMCIS to the (V)6, but *not* sent from the (V)6, appear with a message number in the V6# field, an “X” in the S column, and dots in the MSG TOT field.
- If backlog is confirmed, turn off the OTCIXS interface until the source of the backlog is determined.
- Delete messages to clear backlog.
 - Messages that will be timelate can be deleted, then retransmitted when the problem is corrected– delete in the OUTGOING MESSAGE LOG *and* the (V)6.
 - Messages not sent to (V)6– delete in the OUTGOING MESSAGE LOG WINDOW.
 - Messages sent from JMCIS but not sent from the (V)6– delete in the OUTGOING MESSAGE LOG *and* the (V)6.
- Verify that OTCIXS messages are being received.
- Check the NET CONTROL TIME field.

During periods of heavy use, outgoing messages “stack up” in the (V)6 transmit buffer. The accumulated NO NET time could affect how long it takes for the site to “catch up” when the net controller comes back online.

- Make sure the EMCON status is off in the (V)6. Otherwise, messages can’t be sent.

OTCIIXS-TTY Channel

OTCIIXS-TTY is an optional comms channel. The (V)6 TTY channel is usually connected from the ON-143(V)6 to the USQ 136 teletype. The teletype prints the information passed from the (V)6, and can generate messages for transmission over the OTCIXS/TADIIXS net.

Actively transferring the (V)6 TTY connection from the teletype to JMCIS, or passively tapping into the receive side of the channel, ensures that the OTCIXS/TADIIXS net status can be monitored from within JMCIS.

Information directed from the (V)6 to the teletype includes:

- RCV Guard List from the (V)6 control head
- NO NET CONTROL time
- SID number of the net controller
- Synchronized system (V)6 time

To access the OTCIXS-TTY STATUS window, select WINDOW from the pop-up menu.

Note: The DATA ACCOUNT PRINT option must be active before data can be received. This option is located in DATA LINK PAGE on the (V)6 control head.

Link-11 Channel

JMCIS receives Link-11 data via a serial interface from an EDO box. (Though the EDO box also has an IEEE-488 interface, JMCIS uses only the serial.) Another alternative is an Indian Head serial interface.

The EDO box passively taps the transmit and receive side of Link-11. Link-11 can be run in one of three modes:

- NCS– the ship is the Link-11 controller
- PKT– the ship is a Link-11 picket unit
- RS– the ship is radio silent

JMCIS receives Link-11 data from all participating units (PUs), other than Ownship, if Link-11 and its related components are operational. These components include modem, crypto, radio, and antenna.

JMCIS receives Ownship Link-11 data under the following conditions:

- The Ownship NTDS must be operational.
- Link-11 must be in the NCS or PKT mode.

JMCIS not receiving data from PUs:

1. Contact the Track Supervisor or Tactical Information Controller (TIC) to verify that the Link-11 components are operational.
2. Check the error lights on the EDO box. If an error light is on, the EDO box is preventing the Link-11 data from reaching JMCIS.
3. Check the Link-11 comms channel in JMCIS. (For more information, see *Troubleshooting Software Problems*, described in this chapter.)

JMCIS not receiving data from Ownship:

1. Make sure the Ownship NTDS is operational.
2. Check the Link-11 control panel settings. Ownship Link-11 data will be received only if the unit is in NCS or PKT mode, *not* RS.

DTC Channel

The DTC channel uses a SERIAL interface to support a direct connection between JMCIS and non-JMCIS tactical data processors.

Outgoing messages can be generated by manual transmission, broadcasts, or autoforwarding.

If data is not being sent or received, see *Troubleshooting Software Problems*, described in this chapter.

Low Data Rate (LDR) Channels

Low data rate channels in JMCIS include:

- HIT-BCST
- Link-14

Since these are 75 baud channels, the radio room can switch the patch for an LDR line and attach it to a teletype. Output on the teletype confirms data is being received.

- For more information, see *Troubleshooting Software Problems*, described in this chapter.
- Information pertaining to specific LDR channels is listed below.

HIT-BCST Channel

Please note that the KW-7 crypto is still in use at a few sites. Because of the phasing requirements of the KW-7, CRYPTO PHASE must be selected in the COMMS EDIT window.

- The KW-7/KG-84 sends a phase signal to synchronize with other KW-7/KG-84 units that may be listening. Once this is complete, data must be passed to maintain the signal.
- When the data has been passed, the sync signal “errors out” in the KW-7/KG-84 and is dropped. At this point, the frequency is empty.
- The next phase signal controls the net until *it* stops sending data and drops sync.

If CRYPTO PHASE is not selected, JMCIS *does not* send a series of characters to phase the crypto gear. Therefore, the header on the first message is destroyed during the phasing process.

Link-14 Channel

NATO-format Link-14 is supported by UB versions 2.0.10.1 and above, and by JMCIS versions 2.1.0 and above.

Ownship/Navigation Channels

When updating the position of Ownship, information is passed to JMCIS from one of the following channels:

- SINS
- SRN-19
- SRN-25
- CVNS
- LORAN C
- MX200
- WSN-5
- WRN-6

Though each channel has a window for incoming raw data, this data may not be readable. However, any information in the window—readable or not—verifies that data *is* being received.

If it appears there is no incoming data, confirm the update interval of the navigation channel. Update intervals can be as long as 15 minutes. Use a short interval to test the system, then reset it when data is verified.

The active Ownship interface must be restarted when the NAV update interval is changed. Select RESTART in the COMMUNICATIONS window pop-up menu.

MDX

The MDX interface provides point-to-point data communications—specifically, transmitting track information from one designated site to another. (See EDIT MDX Window in the *UB User's Guide* for details.)

If the interface is not transmitting data, check the following:

- MDX patch Version 5 is loaded.
- The channel is configured properly.
- The route has been established between sites.

- Exact site host names appear in the host table.
- The transmit and receive port designations do not conflict with existing TCP port numbers in the /etc/services file.
- The values for transmitting port at one site match the values for the receiving port at the other site.

5.6.4 BROADCASTS

To troubleshoot a particular broadcast:

- Open the status window for the broadcast. (Broadcast must be ON; use the WINDOW pop-up option.)
- Open the window for the outgoing comms channel.
- Compare message activity.
- Ensure the Commands in the “TO:” fields in the default header are the same as those listed in the Auto-Forward Table.
- When in FOTC mode (Controller or Participant), make sure the correct Receive Guard List in the ON-143(V)6 has been entered.

Notes

Notes

CHAPTER 6: ERROR RECOVERY

Never power off the system without first executing a shutdown. Doing so could cause irreparable damage. If the system has already been brought down incorrectly, refer to *Repairing File Systems*, described in this chapter.

The following topics are covered:

- Basic Error Recovery
- Performance Tips
- Troubleshooting Multi-Monitors
- Identifying Hardware Problems
- Repairing File Systems
- Reporting Problems

6.1 BASIC ERROR RECOVERY

When JMCIS doesn't function as expected, and the SYSTEM SERVICES window (MISC menu) indicates that all processes are running correctly, follow these steps until the problem is corrected.

Access to all System Administration menus and options is required for error recover procedures.

Important! The following procedures are listed according to "risk factor"—that is, from the least to the greatest risk of damaging files or losing data. *Always begin corrective action with the procedure that poses the least risk.*

If these steps don't correct the problem, contact the number listed in *To Report a Problem*, described in this chapter.

Options are unavailable:

Access to options may be restricted for the user's account. Check with Security Manager.

Window hangs or menu option has been disabled:

Select CLOSE ALL from the SYSTEM menu (on the main menu bar). All windows will be cleared from the screen.

Comms interface doesn't work:

1. Select COMMUNICATIONS from the COMMS menu.
2. Highlight the specific interface.
3. Choose RESTART from the pop-up menu.

For more information, see *Troubleshooting Comms Channels and Connections*, described in Chapter 5.)

Map not functional or system prompts to "restart chart":

1. Notify users on remote monitors that their maps will soon close.
2. Select RESTART CHART from the CHARTS menu.
3. Select SYSTEM CHART from the CHARTS menu if the chart doesn't reappear.

Map functions hang:

This process takes approximately 45 seconds and clears all display-oriented functions. The values for the map functions must be reentered when JMCIS starts.

1. Select CLEAN DATAFILES from DATABASE menu on the System Administration menu bar.
2. Select MAP TOGGLES (LOCAL).
3. Click OK.
4. Return to the JMCIS screen.

If the previous specific procedures do not solve the problem, perform the following:

Restart the system:

1. Select EXIT from the SYSTEM menu (on the main menu bar).
2. Click EXIT SYSTEM on the startup screen.
3. Restart with user login.

Reboot the system:

1. Notify users on remote monitors that their maps will soon close.
2. Select REBOOT SYSTEM from the HARDWARE menu on the System Administration menu bar.
3. Restart JMCIS with user login.

Power up/down the system with pointer and keyboard operational:

See Chapter 3, *Operating Guidelines*.

Power up/down the system with pointer frozen:

1. Turn off the monitor and peripherals.
2. Turn off the CPU.
3. Wait approximately 30 seconds.
4. Turn on the monitor and peripherals.
5. Turn on the CPU.
6. Restart JMCIS with the user login.

Reinstall JMCIS:

1. Use the original JMCIS installation tapes if a network installation is not possible.
2. Follow the instructions to reinstall the software. (See Chapter 4, *Software Installation*.)

6.2 PERFORMANCE TIPS

- Double-clicking or repeating commands does not hurry the process.
- When commands are repeated or clicked continually, the system logs them *each time*, thus delaying the process even further.

System is slow:

- Activate required overlays only. If all overlays are activated, it slows the system's performance.
- Close INSET CHART (main menu bar) and use only the SYSTEM

CHART.

6.3 TROUBLESHOOTING MULTI-MONITORS

Any monitor or keyboard fails to respond:

- A reboot may solve the problem.
- Rebooting the computer in a multi-monitor environment means *all* monitors will go down. When working with multi-monitors, contact all users before rebooting.

Monitor is black:

- Make sure the monitor cable is properly connected.
- Make sure the monitor is connected to a power supply and is turned on.
- The video switch may have incorrect input or output, or may be turned off.

Monitor is black with small yellow squares:

- Make sure each monitor is connected to the correct port on the back of the CPU.

Second monitor in a dual-eye configuration is gray:

- Make sure keyboards are connected correctly. This monitor is the second eye of a dual-eye configuration. (See Chapter 2, *Dual-Eye Console*.)

Trackball doesn't respond:

- A reboot usually solves this problem. If it doesn't, try using a different trackball. If it still doesn't work, there may be a wiring problem in the cable.

Keyboard doesn't respond:

- Make sure the keyboard is connected properly.
- The keyboard may be connected properly but the monitor may not “echo” the typed characters to the screen. A reboot usually solves this problem, but can be difficult to perform since the user can't see what's being typed.

6.4 IDENTIFYING HARDWARE PROBLEMS

When the workstation is turned on, the CPU runs a hardware check.

If the hardware check is successful:

- The system boots the device at: SCSI address 0
- b sd(0,0,0) appears, indicating the boot of the primary disk.
- The system displays configuration information, followed by the login prompt.

If the boot fails, there's a disk problem. Refer to the hardware manual.

6.5 REPAIRING FILE SYSTEMS

If the system was brought down unexpectedly (power failure, turned off without proper shutdown, etc.), it's designed to repair the file system when powered up.

- The system should never be powered down while the file system is being repaired. This will cause further damage to the file system.
- If power is fluctuating, leave the system off until power is reestablished.

6.6 TO REPORT A PROBLEM

For immediate assistance, or to report a problem, call the 24-hour hotline at NISE East Det Norfolk:

CONUS: 1-800-869-6413

Overseas: 1-804-399-2762 (collect)

If a problem can't be corrected by the procedures described in this manual, follow these guidelines to report it:

1. Make sure the problem can be repeated.
2. Record:
 - the problem
 - the last steps leading to the problem
 - how often the problem occurs
3. Describe attempts to solve the problem.

Notes